CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

CRIPTOGRAFIA QUÂNTICA: UM ESTUDO DAS PRINCIPAIS VULNERABILIDADES E SUAS CONTRAMEDIDAS.

Johann Lucke

Americana, SP

2014

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Segurança da Informação

JOHANN LUCKE

CRIPTOGRAFIA QUÂNTICA: UM ESTUDO DAS PRINCIPAIS VULNERABILIDADES E SUAS CONTRAMEDIDAS.

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso de Segurança da Informação, sob a orientação da Prof.(a) Me. Graziela Ramos.

Área de concentração: Segurança da informação.

Americana, SP

2014

Johann Lucke

CRIPTOGRAFIA QUÂNTICA:
UM ESTUDO DAS PRINCIPAIS VULNERABILIDADES E SUAS CONTRAMEDIDAS.

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da informação.

Americana, 06 de Dezembro de 2014.

Banca Examinadora:

Graziela Ramos
Mestre
CEETEPS/Faculdade de Tecnologia – FATEC/ Americana

Gustavo Carvalho Gomes de Abreu
Professor
CEETEPS/Faculdade de Tecnologia – FATEC/ Americana

Raul Paiva de Oliveira
Professor
CEETEPS/Faculdade de Tecnologia – FATEC/ Americana

Lucke, Johann

L973c Criptografia quântica: um estudo das principais vulnerabilidades e suas contramedidas. / Johann Lucke. – Americana: 2014.

46f.

Monografia (Graduação em Tecnologia em Segurança da informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Me. Graziela Ramos

1. Segurança em sistemas de informação I. Ramos, Graziela II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

RESUMO

Este trabalho apresenta como seu objetivo a temática da criptografia, sua origem e desenvolvimento, neste se parte da era clássica, então para seu aperfeiçoamento à criptografia moderna, e além para sua recente transformação na criptografia quântica. Dessa forma, para uma melhor compreensão desta progressão, é discutido também a criptoanálise, seus métodos antigos e modo de análise moderno, além da criptografia moderna, seus princípios e alguns de seus processos de proteção. É também discutido os princípios da física quântica e como eles influenciam no funcionamento da computação quântica. Diante disso, a criptografia quântica é apresentada, assim como seu funcionamento e protocolos, e finalmente as vulnerabilidades deste novo método de proteção à informação no ambiente quântico, as quais foram descobertas e trabalhadas pelo Instituto de Computação Quântica de Waterloo, o mesmo que também apresenta algumas potenciais soluções para tais fragilidades. Por último, discute-se o impacto que toda esta nova área tecnológica tem para com a segurança da informação e seus profissionais.

Palavras-chave:
Criptografia, Criptoanálise, Computação Quântica, Vulnerabilidades, Segurança.

ABSTRACT

This work presents as its goal the theme of encryption, its origin and development, since its classic age, to its improvement into the modern cryptography, and also its recent transformation into quantum cryptography. This way, for the best understanding of such progression, is also discussed cryptanalysis, its ancient and modern ways of analysis, modern cryptography, the principles and some of the protection processes. It's also presented the principles of quantum physics and how those affect the operation of quantum computers. With that in mind, the quantum cryptography is then introduced, also its operation and protocols, and then finally the vulnerabilities of this new method to protect the information in the quantum environment, which were discovered and worked by the Institute for Quantum Computing in Waterloo, the same presenting some potential solutions for such flaws. And at last, it's discussed the effect that all this new technology area has towards information security and its professionals.

Keywords:
Cryptography, Cryptanalysis, Quantum Computing, Vulnerability, Security.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

OTP - *One-time Pad* (cifra/chave de uso único)

RSA - Rivest Shamir Adlerman, sobrenomes dos criadores

AES - *Advanced Encryption Standard* (Padrão de Criptografia Avançada)

DES - *Data Encryption Standard* (Padrão de Criptografia de Dados)

3DES - *Triple Data Encryption Standard* (Triplo Padrão de Criptografia de Dados)

RC4 - *Ron's Code* 4 (Código 4 do Ron)

PGP - *Pretty Good Privacy* (privacidade bastante boa)

BB84 - Bennett Brassard 84, sobrenomes dos criadores e ano de criação

E91 - Ekert 91, sobrenome do criadore e ano de criação

BBM92 - Bennett Brassard Mermin 84, sobrenomes dos criadores e ano de criação

B92 - Bennett 92, sobrenome do criadore e ano de criação

APD - *Avalanche photodiode* (Avalanche Fotodiodo)

SUMÁRIO

1.INTRODUÇÃO

Os homens em suas diferentes culturas sempre possuíram a ambição pelo conhecimento do outro, motivo pelo qual foram sendo criados processos para a proteção do mesmo, sendo um destes processos a criptografia. Este trabalho tem como objetivo geral, primeiramente apresentar ao leitor um breve - porém compreensivo - estudo sobre a história da criptografia, voltada para a computação, ou mais especificamente para a proteção da informação na computação, seu surgimento e adaptação da era clássica para a moderna e até os tempos atuais, além de apresentar o desafio proposto pela criptoanálise. Estes conceitos são introduzidos ao longo dos primeiros três capítulos.

Uma vez que tais preceitos estejam claros e o leitor encontre maior facilidade em compreender o *Modus Operandi* da criptografia e criptoanálise, é apresentada, de maneira simplificada no capítulo 4, uma explicação sobre o funcionamento da computação quântica e seus princípios baseados na física quântica. Como mencionado, estes são feitos em um breve estudo, devido à maioria das explicações detalhadas serem baseadas na matemática (o que não é a área de foco deste trabalho), possibilitando a compreensão por aqueles que se interessam pela temática, mas se apresentam leigos à compreensão de tais cálculos.

Deste modo, o leitor pode compreender melhor o sistema em que a criptografia quântica opera e como ela o faz, o que é apresentado no capítulo 5, ainda que no seu atual estado de desenvolvimento. São apresentados os principais protocolos da mesma assim como seu funcionamento. Enquanto que no capítulo 6, são detalhadas algumas problemáticas desta tecnologia, vulnerabilidades apresentadas e trabalhadas pelo Instituto de Computação Quântica de Waterloo, assim como análises e possibilidades de soluções apresentas pelo mesmo.

Por fim, o último capítulo retoma as informações apresentadas em referência ao impacto gerado no cenário da segurança da informação como um todo.

2.CRIPTOGRAFIA CLÁSSICA

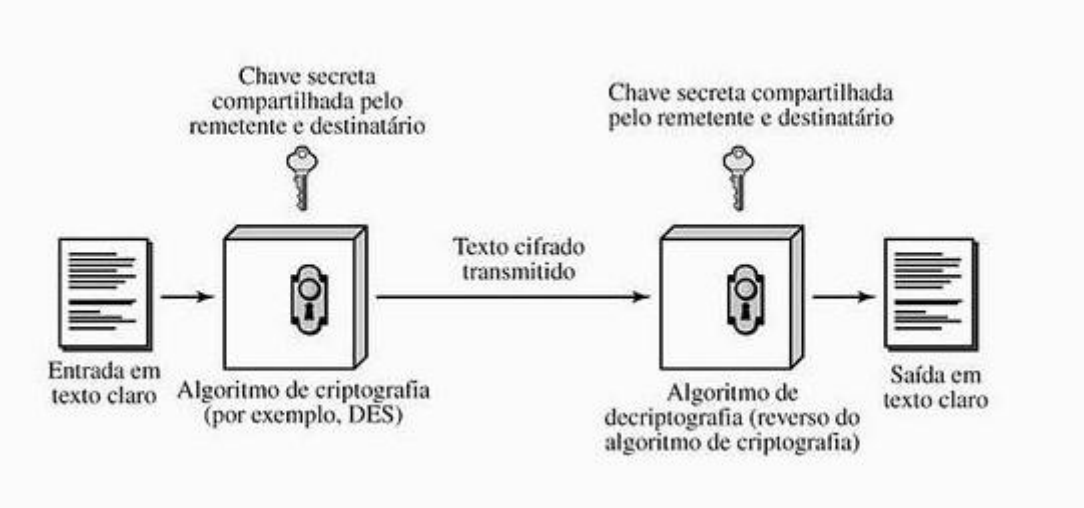
2.1.Introdução à criptografia

Singh (2000) e Stallings (2007) definem a palavra criptografia como um termo vindo do grego em que *kryptós* é oculto e *graphein* é escrita. A criptografia é, dessa forma, considerada uma ciência que visa ocultar o que se tem escrito e os métodos utilizados para este fim são técnicas chamadas de cifras. As chamadas cifras são procedimentos que utilizam chaves ou senhas, de modo tanto a codificar quanto a descodificar uma informação, que pode ser uma escrita, uma mensagem ou até mesmo uma sequência de números, como demonstra a Figura 1.

Uma vez gerado um texto cifrado ou codificado, o mesmo pode ser enviado por um meio inseguro, pois apenas aqueles que conhecem o meio para desvendar sua codificação conseguirão compreender o conhecimento ocultado pela cifra com facilidade. Singh (2000) apresenta também a técnica anterior a esta chamada de Esteganografia (do grego, *steganos* significa coberto), na qual a existência da mensagem e não seu conteúdo era oculto, visando passar despercebida por um possível interceptador no meio desprotegido de envio. Em seu momento de origem, ambas as técnicas eram utilizadas em conjunto de forma a dificultar ainda mais a obtenção da informação escondida.

Ainda em seu livro, Singh (2000) explica que o primeiro registro que se tem sobre o uso de um sistema criptográfico é datado da época das Guerras da Gália (58 AC. a 52 AC.), em que o próprio Júlio César utilizava um método criptográfico em suas mensagens, conhecido hoje em dia como cifra de deslocamento de César, ou simplesmente, cifra de César. Em suas mensagens, ele escrevia ordens e informes que viriam a ser enviados a suas tropas e comandantes, no entanto, ele trocava cada letra da mensagem por outra letra localizada três casas adiante no alfabeto, exemplificado na Figura 2.

Figura 1 – Modelo simplificado da criptografia convencional.



Fonte: (STALLINGS, 2007, p. 18)

Assim, uma mensagem como "*VENI, VIDI, VICI*", do latim "eu vim, eu vi, eu venci", usada também por César anos depois, seria enviada como "YHQL, YLGL, YLFL", e não seria compreendida por algum inimigo que viesse a interceptá-la, garantindo a segurança da informação enviada.

Figura 2 – Cifra de César aplicada a uma mensagem curta

Alfabeto original	a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfabeto cifrado	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Texto original	v e n i, v i d i, v i c i
Texto cifrado	YHQL, YLGL, YLFL

Fonte: (SINGH, 2000, p.27)

2.2.Transposição e Substituição

Ainda sobre a cifra de César, Singh (2000) informa que esta pertence a um ramo da criptografia clássica que é chamado de técnicas de substituição. Neste tipo de técnica as letras, símbolos ou mesmo palavras inteiras de um texto são substituídas por outras utilizando algum padrão de substituição pré-determinado entre o remetente e o receptor. Estes padrões podem ser do mesmo alfabeto, ainda

que todo misturado, ou de outro alfabeto, e até mesmo apenas símbolos aparentemente desconexos. Outro ramo existente são as técnicas de transposição, nas quais a mensagem é literalmente embaralhada de forma a se tornar um anagrama, mas assim como na substituição é necessário ter um acordo prévio entre, o remente e o emissor, quanto à forma como ocorrerá este embaralhamento, caso contrário a mensagem se torna indecifrável e perde seu propósito.

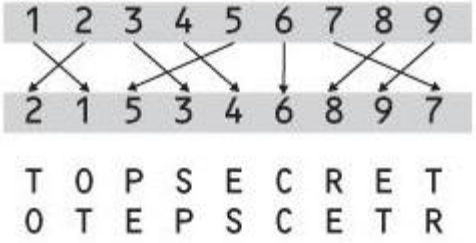
Figura 3 – Exemplo do processo de substituição.

Fonte: (Autoria própria)

Diversas técnicas foram criadas desde a cifra de César, mas todas seguem um destes ramos ou mesmo ambos, de forma a reforçar a segurança da cifra e assegurar a proteção da informação.

A Figura 3 apresenta um exemplo de cifra de substituição na qual se utiliza o alfabeto latino ou romano substituindo uma letra por outra do próprio alfabeto. Desta forma modifica-se a mensagem a outra ininteligível.

Figura 4 – Exemplo do processo de transposição.



Fonte: (Autoria própria)

Já a Figura 4 traz um exemplo de cifra de transposição, em que a mensagem recebe números referentes a cada letra, que são então misturados numa nova ordem, o que transforma a mensagem em um anagrama.

Estes métodos às vezes utilizam números ou palavras completas, como na cifra de Vigenère, que tem um funcionamento similar à cifra de Cesár, porém modificando para cada letra a chave conforme o quadrado de Vigenère, apresentado na Figura 5.

Figura 5 – Quadro de Vigenère.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
04	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
06	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
07	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
08	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
09	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: (Singh, 2000, pag. 66 – Modificado pelo autor)

No caso da troca de palavras, uma mensagem como “ATACARBASESUL”, utilizando uma chave como “LIMAOLIMAOLIM” (palavra limão repetidas vezes), teria como mensagem codificada “LBMCOCJMSSDCX”. Em casos numéricos geralmente há o uso de números com tamanhos variados, às vezes curtos, às vezes muito extensos.

2.3.*One-time Pad*

One-time pad (OTP) é um método de uso de chave única, usado por alguns algoritmos modernos, Singh (2000) explica que se trata de uma derivação da cifra de Vernam, cifra a qual codificava a mensagem usando uma chave em fita perfurada. A OTP é realizada com o emissor e o receptor possuindo uma quantidade de chaves compartilhada apenas entre ambos, estas chaves sendo todas aleatórias, porém sortidas na mesma ordem, de modo que a cada transmissão ambos usem a mesma chave, mas na transmissão seguinte utilizem outra, e assim por diante, o que impede a criptoanálise através da comparação de diversas mensagens interceptadas.

O método OTP se baseia em transposição e substituição também, porém o diferencial é esta geração e compartilhamento de chaves que são usadas uma única vez. Ele foi muito utilizado ao longo de todo o século XX, principalmente em períodos de guerra.

3.CRIPTOANÁLISE

3.1.Análise de frequência

Diante destas formas de ocultar a informação outra ciência foi criada também no campo da criptografia, a chamada criptoanálise, cujo propósito é justamente descobrir meios de revelar a informação escondida por uma cifra, mesmo sem se ter o conhecimento da cifra ou chave utilizada. Singh informa que, apesar do termo ter sido criado apenas em 1920 por William Friedman, a criptoanálise já havia sido criada muito antes por um árabe de nome Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi, o qual viveu no século IX e foi o pioneiro da criptoanálise, tendo descoberto, através de constantes estudos matemáticos, um método de desvendar as cifras, que veio a ser conhecido como análise de frequência.

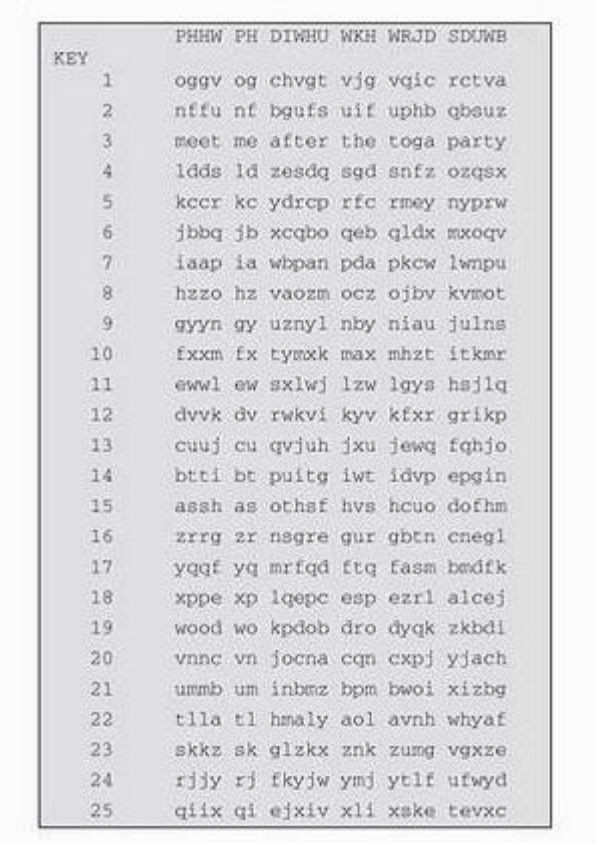
A análise de frequência é um modo que consiste na avaliação do texto cifrado e na determinação de padrões existentes na mesma, os quais levam a descobrir a cifra e até mesmo a chave utilizada. Um analista percebe quais letras ou símbolos que são repetidos com maior ou menor frequência que os demais no texto codificado, ou mesmo uma sequência ou junção destes que se repete mais comumente, e então os compara a padrões comuns existentes nas possíveis linguagens em que a mensagem pode estar escrita, assim ele vai aos poucos descobrindo possibilidades de uma letra ou símbolo ser outro e, após ter algum bom material revelado, consequentemente decifra a cifra e/ou chave. Apesar de parecer fácil, a maioria das análises de frequência demora um tempo prolongado, visto que, às vezes, as análises levam a mais de uma possibilidade de tradução, o que cria a dúvida de qual das traduções é o conteúdo real. Dessa forma, às vezes se faz necessário interceptar mais de uma mensagem codificada para poder fazer um comparativo entre elas, o que então leva à certeza quanto ao conteúdo revelado. Vários métodos de análise foram criados ao longo dos séculos para diferentes cifras, como, por exemplo, a codificação de Huffman – que não será aprofundada neste trabalho -, a qual cria uma árvore de probabilidades, a chamada árvore de Huffman,

na qual se analisa cada símbolo como mais provável, ou menos provável quando em junção a outros símbolos e assim vai medindo parte a parte até enfim revelar uma ou mais palavras completas e, após isso, o texto.

3.2.Força Bruta

Há uma alternativa à técnica de análise de frequência, que utiliza menos raciocínio e análise, e é chamada de ataque de força bruta. Utilizando-se desta técnica, um analista é capaz de encontrar com certeza a cifra ou chave, porém, o tempo levado é, em geral, grande demais para se considerar. A técnica se baseia apenas em tentativa e erro, ou seja, em ter cada possível combinação testada em um método de busca até que a correta seja encontrada.

Figura 6 – Criptoanálise pela força bruta da cifra de César.



KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Fonte: (STALLINGS, 2007, p. 23)

Em tempos distantes, diversas pessoas o faziam simultaneamente de forma a reduzir o tempo gasto, mas, nos tempos atuais, o poder de processamento de diversos computadores pode ser unido de forma a acelerar ainda mais o processo. De qualquer forma, independente da técnica usada, um detalhe permanece constante: descobrir um conteúdo escondido demora tempo e, às vezes, tempo demais para se considerar a tentativa.

Este tempo excessivo necessário para quebrar uma cifra é o que garante a segurança de muitos algoritmos modernos, visto que mesmo os computadores mais poderosos demorariam muitos anos para quebrar uma única chave, tornando inviável esta técnica para os algoritmos mais comuns.

Como demonstrado na Figura 6, a cifra de César teria sua mensagem testada com as 25 possibilidades de chave, e então cada resultado seria verificado para se checar se seria possível considerá-lo válido ou não como o texto real.

4.CRIPTOGRAFIA MODERNA

4.1.Criptografia na computação

Na era moderna, visto que já não são utilizados com frequência cartas ou mensageiros, a criptografia teve de ser adaptada ao meio mais frequente de uso da informação, o ambiente computacional. Diversos algoritmos foram criados neste meio, de forma a ter a informação sempre protegida e a dificuldade da criptoanálise, em desvendar o conteúdo oculto, cada vez mais elevada. A criptografia, dessa forma, encontra-se vinculada a diversos atributos que auxiliam na manutenção da segurança da informação. Tais atributos procuram garantir certos aspectos que são descritos por Stallings (2007) como autenticidade, confidencialidade, disponibilidade e integridade.

Autenticidade: Aspectos os quais garantem que a informação foi de fato emitida pela fonte informada, ou seja, uma mensagem enviada por uma pessoa, de fato foi enviada por esta e não por outra se passando por ela.

Confidencialidade: Aspectos nos quais a informação se encontra restrita apenas àqueles com autoridade ou real necessidade de terem acesso a ela, mantendo-se sigilosa a todos os demais.

Disponibilidade: Aspectos que garantam que a informação encontrar-se-á disponível a quem a busque. A disponibilidade, no entanto, é apenas por aqueles que possuem permissão legitima do proprietário da informação para seu acesso.

Integridade: Aspectos que garantam que a informação mantenha as propriedades atribuídas pelo proprietário da informação de forma não manipulada por terceiros. Tanto em seu estado inicial quanto em futuras modificações, ou mesmo na destruição de tal informação.

A criptografia consegue facilitar na preservação de vários destes atributos, com atenção principal à autenticidade e à confidencialidade, de forma a garantir cifras que gerem maiores benefícios e menores custos e riscos aos proprietários das informações. Os usos atuais de criptografia variam, como para codificar mensagens, fazer o mesmo com códigos-fonte, partições de disco, arquivos e muitos outros, mas é inegavelmente de uso obrigatório no mundo atual, onde informação é poder.

Outro detalhe a se ressaltar na atual era da computação, é que as técnicas de criação de chaves baseadas em transposição e substituição se tornaram obsoletas, visto que o poder de processamento dos atuais computadores é capaz de quebrar o código e desvendar a chave em um tempo muito reduzido em comparação às eras anteriores. Dessa forma, as técnicas mais modernas começaram a usar cálculos matemáticos, como por exemplo, o RSA (Rivest Shamir Adlerman, sobrenome dos criadores) que se aproveita da teoria clássica dos números primos e utiliza um processo de geração de chave com base em extensos números primos aleatórios, tornando mesmo o mais poderoso computador, em termos de processamento, incapaz de quebrar sua cifra em margem de tempo aceitável.

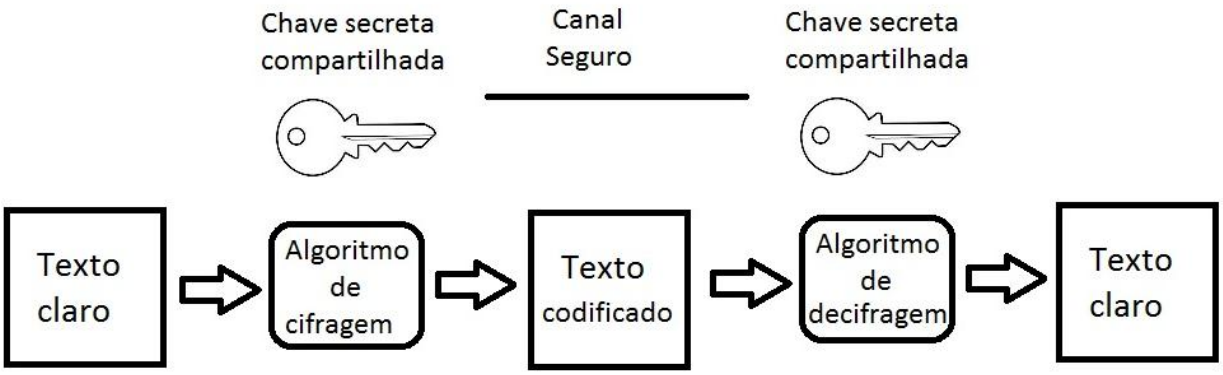
4.2. Algoritmos Simétricos e Assimétricos

Na chamada criptografia moderna, Singh (2000) demonstra haver duas categorias em relação às chaves, sendo chamadas de algoritmos de chave simétrica e de algoritmos de chave assimétrica, nos quais a diferença se dá no número de diferentes chaves utilizadas e no modo como elas são manuseadas, o que modifica por completo o processo e o uso.

Os algoritmos de chave simétrica, também conhecidos como criptografia de chave única e criptografia de chave privada, são o uso mais comum da criptografia e funcionam a base de um algoritmo que possui uma única chave secreta para fazer e desfazer a codificação do texto. Em um sistema desses, ambos, o receptor e o emissor, têm estabelecida uma chave privada através de um canal seguro, ou em alguns casos mais modernos, como o *One-time pad*, mantendo-se conhecida apenas pelos dois participantes desta comunicação. O método de funcionamento é o mesmo utilizado por cifras mais antigas no qual o emissor envia a mensagem

criptografada com esta única chave secreta através de um meio inseguro. O receptor, uma vez possuindo o conhecimento da mesma chave, utiliza-a para decifrar a mensagem enviada e ver seu conteúdo, como demonstrado na Figura 7. Dentre os algoritmos modernos mais comuns que utilizam este sistema, podemos citar o AES (*Advanced Encryption Standard*), o DES (*Data Encryption Standard*), o 3DES (*Triple Data Encryption Standard*) e o RC4 (*Ron's Code 4*).

Figura 7 – Demonstração do funcionamento de algoritmos simétricos.



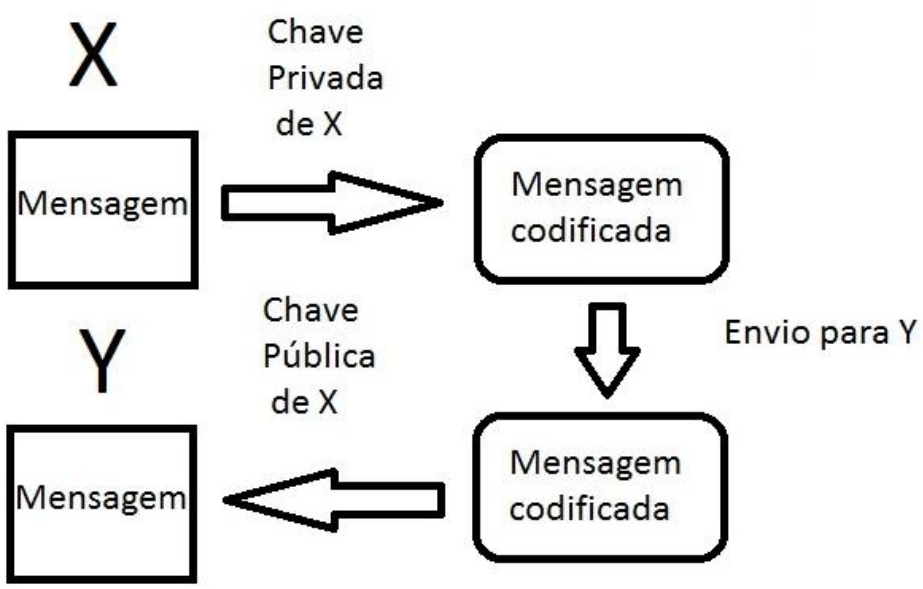
Fonte: (Autoria própria)

Por outro lado, os algoritmos de chave assimétrica, conhecidos também como criptografia de chave pública, utilizam duas chaves para o seu funcionamento, uma sendo mantida como secreta e a outra sendo deixada pública para cada participante no canal de comunicação. Cada emissário e receptor, possui a sua própria chave privada e o conhecimento das chaves públicas dos demais participantes. Ou seja, tanto o receptor quanto o emissor possuem cada um, duas chaves, uma que pode ser de conhecimento público e outra que permanece conhecida apenas por eles mesmos. Uma chave pública só pode ser aberta pela chave privada da mesma pessoa e vice-versa, assim seu funcionamento ocorre dependendo de qual atributo da segurança da informação se busca utilizar, como será explicado adiante.

Autenticidade – Para ter-se como autenticado que a pessoa X enviou uma mensagem à pessoa Y, X codifica seu conteúdo utilizando sua própria chave privada

e a envia a Y pelo meio inseguro. Y, ao receber a mensagem codificada terá de utilizar a chave pública de X, a única que revelará o conteúdo da mensagem. Como X é o único que conhece sua própria chave privada, uma vez que a mensagem seja decifrada usando sua chave pública, Y tem certeza de que ele de fato enviou a mensagem. Este processo, exemplificado na Figura 8, tem, no entanto, uma vulnerabilidade que se deve ao fato de qualquer um dentro da autorização de acesso às chaves públicas poder vir a decifrar a mensagem com a chave pública de X, uma vez que a tenha adquirido. Dessa maneira, não há confidência para com o conteúdo.

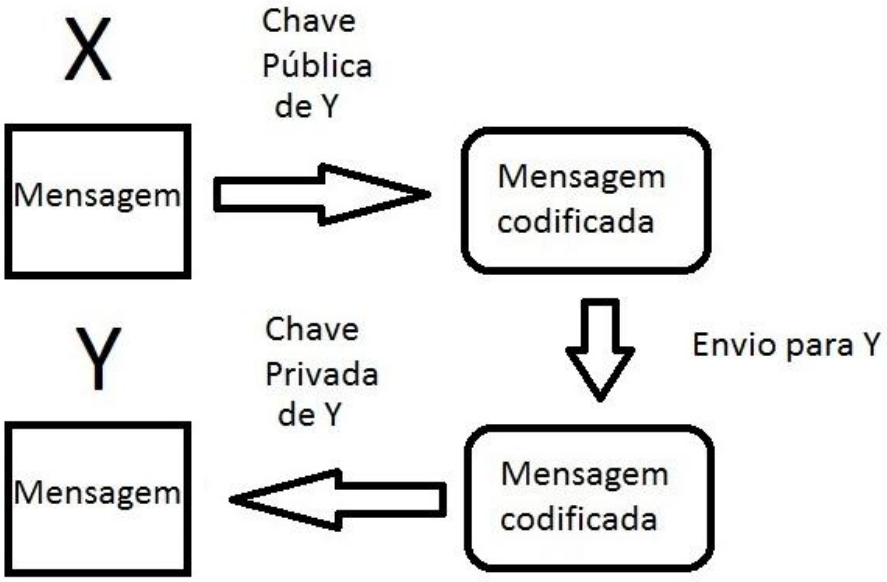
Figura 8 – Demonstração do método de autenticidade em algoritmos assimétricos.



Fonte: (Autoria própria)

Confidencialidade – Para se utilizar da confidencialidade, a mesma pessoa X envia uma mensagem a Y, dessa vez utilizando a chave pública de Y para codificar a mensagem. Uma vez recebida a mensagem por Y, apenas a chave secreta da mesma será capaz de revelar o conteúdo, assim ninguém além de Y saberá o que há na mensagem. Porém, este processo, exemplificado na Figura 9, também possui uma vulnerabilidade, visto que qualquer um pode enviar a Y uma mensagem se passando por outra pessoa.

Figura 9 – Demonstração do método de confidencialidade em algoritmos assimétricos.



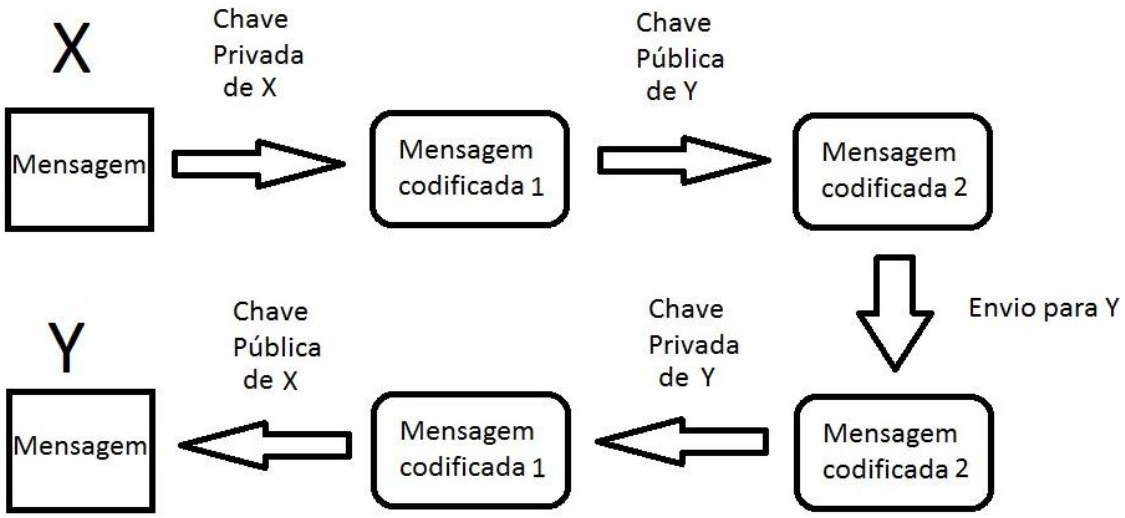
Fonte: (Autoria própria)

Autenticidade e confidencialidade – Neste último processo, X busca enviar a Y uma mensagem, mas ele o fará de modo a garantir de fato o envio e de modo que apenas Y seja capaz de descobrir o que há escrito. X codifica a mensagem utilizando a sua chave privada e então a codificando novamente com a chave pública de Y. O mesmo, ao receber a mensagem vinda de X, terá de decodificar usando sua própria chave privada e, em seguida, usar a chave pública de X. Dessa forma, Y terá certeza que a mensagem é de X e que mais ninguém a viu. Este funcionamento também possui vulnerabilidades, visto que é mais lento que ambos os anteriores devido à necessidade de duas codificações e de duas decodificações. Este processo é demonstrado na Figura 10.

Além das vulnerabilidades apresentadas, todos os processos possuem ainda outra fragilidade. Caso algum terceiro venha a modificar os registros de senhas públicas por senhas que apenas ele possua as versões privadas, ele será capaz de descobrir o conteúdo das mensagens enviadas por qualquer um dos métodos. A fraqueza principal do algoritmo de chave pública se dá no aspecto da integridade, uma vez que sempre há a possibilidade do fator humano com segundas intenções.

Nos algoritmos modernos mais conhecidos que utilizam este modo, constam o PGP (*Pretty Good Privacy*) e o RSA, ou seja, algoritmos mais lentos que os de chave única, mas que demonstram maior segurança.

Figura 10 – Demonstração do método de autenticidade e confidencialidade em algoritmos assimétricos.



Fonte: (Autoria própria)

4.3.Criptoanálise moderna

Em confronto às técnicas recentes de criptografia, a criptoanálise permanece com poder contra cifras e algoritmos mais fracos, mas no que diz respeito aos métodos mais fortes, ela se encontra incapaz de competir utilizando o poder de processamento atual.

Dos métodos mais poderosos atualmente utilizados, um supercomputador necessitaria de centenas de anos para quebrar uma única chave. Tal processo demonstra a ineficiência da técnica de força bruta. Uma análise de frequência se encontra igualmente incapaz de determinar um padrão, visto que os algoritmos mais eficientes se utilizam de teoremas matemáticos, e não algum tipo de recombinação da mensagem.

Há, porém, a chamada Lei de Moore, lei que estabelece o crescimento do número de transistores em chips em 100% a cada 18 meses, e que tem mostrado que, em um tempo futuro, mesmo algoritmos com chaves grandes como o RSA serão incapazes de garantir a segurança de suas chaves.

Uma realidade cada vez mais próxima que apresenta potencial ainda superior é a computação quântica, a qual teoriza um poder computacional muito mais elevado em relação aos computadores atualmente existentes, de forma a colocar em risco os protocolos de criptografia atuais.

5.COMPUTAÇÃO QUÂNTICA

5.1.Física Quântica

Conforme descreve Pessoa Jr. (2003), a física quântica, também conhecida como mecânica quântica, ou teoria quântica é um ramo da física que não se deu origem por um autor, mas por diversas conclusões de diversos autores dos séculos XIX e XX, ainda que os principais estudos referentes possam ser atribuídos a físicos como Max Karl Ernst Ludwig Planck – criador da Lei de Planck da Radiação –, Niels Henrick David Bohr – o qual demonstrou a teoria de Planck no modelo atômico de Rutherford -, Werner Karl Heisenberg – criador da Lei do princípio de incerteza – e Erwin Rudolf Josef Alexander Schrödinger – criador do experimento mental conhecido como Gato de Schrödinger. O termo, o qual recebeu o nome por Max Born – criador da Lei de Born - em 1924, se refere a um estudo da física voltado ao estudo de matéria e partículas em níveis atômicos e subatômicos, na escala dos Angstrons 1 Å = 10^{-10} metros = 0,0000000001 metros, situações nas quais a física clássica nem sempre é exata.

Dentre os grandes avanços da física quântica, encontra-se o princípio de dualidade onda-partícula, atribuído em especial à luz, ou mais especificamente aos fótons, os quais são base para a tecnologia da computação quântica.

5.2.Princípios da Física Quântica

Há dois princípios fundamentais na compreensão da física quântica com o objetivo de explicar a computação quântica. São eles, o problema de medição, o qual pode ser entendido através do experimental mental paradoxal de Schrödinger, e o princípio de incerteza de Heisenberg, ou princípio da indeterminação na física clássica de ondas, que estabelece a possibilidade de uso do fóton como unidade básica de informação.

O problema de medição, explica Pessoa Jr. (2003), é explicável pelo experimento do gato de Schrödinger onde:

> Um gato é fechado dentro de uma câmara de aço junto com um pouquinho de uma substancia radioativa, que tem uma probabilidade 50% de acionar um detector dentro de certo intervalo de tempo. Ligado a este detector há um dispositivo diabólico que funciona de tal maneira que, se o detector fosse disparado, o gato seria morto, enquanto que ele permaneceria vivo se nenhuma radiação fosse detectada no intervalo de tempo. (PESSOA JR, 2003, Vol. 1, p. 61.)

Este é o modo como é descrito o estado de um átomo quando não se encontra em uma superposição, ou seja, um estado que é indeterminado se não medido. No experimental mental paradoxal, o gato pode estar tanto vivo quanto morto, não havendo modo de medir ou analisar sem que se tenha alguma interação com a câmara de aço fechada, no caso abrindo-a para observar, ação tal que geraria um chamado colapso de estado, o que viria a criar uma determinação de estado, ou seja, no caso do gato, a verificação se ele está vivo ou morto, não mais uma superposição onde ambos são possíveis simultaneamente. Esta é uma visão válida apenas a matérias em estado microscópico fora da física clássica, visto que se realiza em uma escala macroscópica, ou seja, qualquer observação de terceiros não geraria tipos de efeito sobre o resultado do experimento, sendo tais resultados, no entanto, meramente teóricos, uma vez que não é possível observá-lo ocorrer.

Este conceito de algo ser real quando não se é capaz de observá-lo é conhecido como regra da correspondência, na qual se estabelece uma incapacidade de se medir o estado de um material quando observado, sem que este seja finito, enquanto que uma matéria não observada pode se encontrar em infinitas possibilidades.

O outro conceito base para a computação quântica é o principio de incerteza de Heisenberg, também conhecido como princípio de indeterminação, o qual é descrito separadamente por Pessoa Jr. (2003) como a interpretação de que um elétron tem sua posição e momento (nível energético e forma dos orbitais no elétron) definidos, no entanto, um destes permanece desconhecido. Este princípio diz que não é possível determinar com precisão ambos os valores, apenas um. O

experimento utilizado para tal determinação consiste em duas partes, uma para determinar a posição e uma para o momento.

Quando buscando encontrar a posição, é necessário iluminar o elétron, e quanto menor o comprimento de onda de luz utilizado, maior precisão terá o resultado. Quando o elétron tem incidido em si um fóton bastante energético, o qual tem energia proporcional à frequência de luz, que é inversamente proporcional ao comprimento de onda, sua posição se torna determinável. No entanto, ao ter o fóton incidido ao elétron, parte da energia é transferida, acelerando o elétron e tornando impossível analisar seu momento.

Assim ao tentar determinar o momento, é necessário antes calcular seu número quântico, determinado pela massa dos nêutrons, a carga dos elétrons junto a constante de permissividade do vácuo e a constante de Planck. Porém, em momento algum, será possível determinar a posição do elétron, havendo apenas a possibilidade de suposição ou especulação sem grande precisão. Dessa maneira, a característica deste princípio é o fato dele se manifestar na forma do produto de incertezas. Quanto maior a precisão em uma medida, menor a precisão na outra.

Estes dois princípios juntos formam um sistema quântico, no qual sempre há interação não determinável entre aquele que observa e o que é observado, sistema o qual é aproveitado na criptografia quântica.

5.3.Emaranhamento quântico

O Emaranhamento quântico, ou estado quântico emaranhado, é uma situação cujo funcionamento ainda não foi completamente entendido por seus pesquisadores, no entanto os efeitos que produz já são bem claros. Pessoa Jr. (2003), explica que nesse fenômeno é possível “entrelaçar” duas partículas de forma que mesmo que elas sejam desconectadas e distanciadas, ainda haja uma conexão entre elas e, caso gere alteração em uma destas, causará uma alteração na outra. Mesmo numa simples medição, é impossível analisar e mencionar uma, sem a menção da contra parte.

Como esta conexão subatômica funciona, mesmo com as partículas estando a centenas de quilômetros uma da outra, ainda é um mistério na física quântica, porém, essa reciprocidade entre as partículas é algo confirmado e aproveitado dentro da física quântica, computação quântica e também agora na criptografia quântica.

5.4.Computação quântica

Em seu trabalho, Brumatto (2010) descreve a computação quântica como simplesmente o próximo passo na evolução natural da computação para ultrapassar as barreiras impostas pela, em suas palavras, a “velocidade da luz no processamento da informação e a dimensão da ordem de grandeza atômica, no tamanho dos componentes em um chip.” (Brumatto, 2010, pag. 1). Ou seja, mesmo diante da Lei de Moore quanto à taxa de crescimento, há um limite de tamanho físico quanto à medida que um chip poderia ter, e um limite virtual em seu poder de processamento de informações e capacidade. Limites os quais só podem ser superados com a criação de, como dito por Brumatto, novos paradigmas na construção de hardwares, o que envolveria a computação quântica.

Enquanto a computação moderna, como descreve Deutsche (1985), se baseia num sistema que computa com um número determinado e imutável de estados de entrada e estados de saída, ou seja, recebe apenas certo número de informação a computar e é capaz de obter apenas este mesmo certo número de resultados as requisições, o computador quântico possui uma quantidade desconhecida de estados de entrada, sendo indeterminável ao usuário que busca descobrir este número, mas sabendo apenas que a quantidade de estados de saída será proporcional à quantidade de entradas. De modo simplificado, enquanto os computadores modernos podem receber e processar apenas um número determinado de instruções e tarefas simultaneamente, os computadores quânticos podem fazê-lo com números indeterminados.

Brumatto (2010) explica que a base da computação quântica é o Qubit, ou um bit quântico. Enquanto um bit na computação moderna possui apenas dois estados fundamentais sendo eles 0 ou 1, o bit quântico possui os dois estados

fundamentais e uma superposição de ambos, podendo ser 0, 1 ou ser 0 e 1. Assim, o Qubit segue uma proporção onde um sistema com n Qubits possuirá 2^n estados fundamentais. Dessa forma enquanto 3 Qubits operam em 8 estados fundamentais, 4 Qubits em 16, 5 Qubits em 32 e assim exponencialmente.

Tabela 1 – Correspondência entre bits e Qubits

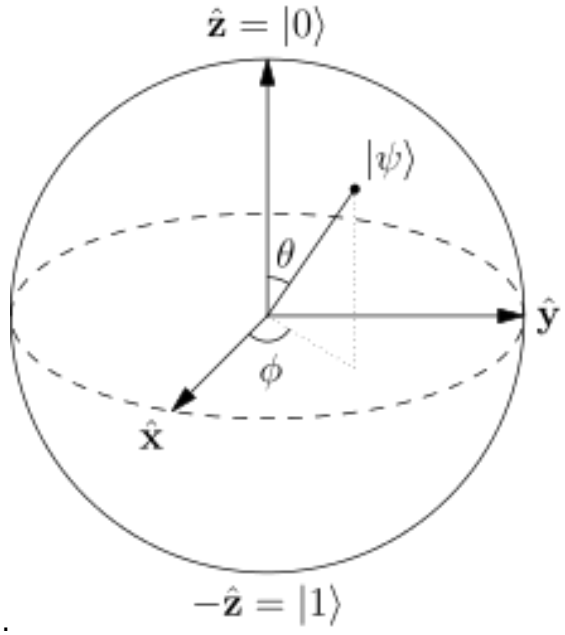
Qubits	Correspondente em bits
2 Qubits	4 bits
3 Qubits	8 bits (1 byte)
4 Qubits	2 bytes
5 Qubits	4 bytes
6 Qubits	8 bytes
7 Qubits	16 bytes
8 Qubits	32 bytes
9 Qubits	64 bytes
10 Qubits	128 bytes
20 Qubits	131.072 bytes
30 Qubits	134.217.728 bytes
40 Qubits	137.438.953.472 bytes
43 Qubits	1.099.511.627.776 bits (1 tebibyte)

Fonte: (autoria própria)

Segundo Brumatto, “As operações em um computador quântico ocorrem através de portas quânticas sobre estados quânticos do sistema, as medidas são obtidas com base na distribuição probabilística na descrição do estado.” (Brumatto, 2010, p. 3). Em outras palavras, enquanto num computador moderno cada novo bit adiciona apenas uma única capacidade de informação ao conjunto, cada novo Qubit dobra a capacidade de informação do mesmo. Isso se deve a cada porta lógica quântica interagir como todos os Qubits, e não em operações isoladas por bit. Ele exemplifica isso de modo simples, explicando que uma porta lógica clássica ao receber dois bits, possuirá quatro entradas, mas apenas duas saídas, enquanto que na quântica, haverá quatro entradas e quatro saídas. Assim, uma operação que num computador atual poderia demorar muitos anos, poderia ser feita num computador quântico em questão de minutos.

Brumatto (2010) ainda explica que há cinco tipos de portas NÃO na computação quântica, a porta Pauli (X), a controladora (CNOT), a Hadanard (H), a de fase (S) e a $\pi/8$ (T), enquanto que na lógica binária clássica há apenas um tipo de porta NÃO que opera com 1 bit e tem como função apenas inverter a entrada, fazendo com que um 0 que seja recebido saia como 1 e vice-versa.

Figura 11 - Um Qubit representado por uma Esfera de Bloch



.

Fonte: (CARVALHO, VIRGINIA, 2005, p.11)

Na lógica quântica, a posição, ou estado do Qubit, deve ser pensada como num eixo tridimensional com base, altura e profundidade. Cada porta destas possui como finalidade causar uma rotação, inversão ou recolocação do Qubit, ou dos próximos Qubits que a atravessarem dependendo do resultado gerado pelo Qubit anterior. Ainda que seus funcionamentos específicos sejam explicados por fórmulas físicas e cálculos matemáticos, as quais não serão demonstradas neste trabalho por fugir do proposito inicial, é possível se ter uma ideia da variação de posições que podem ser geradas a se ver a esfera de Bloch, demonstrada na Figura 11, como explicam Carvalho e Virginia (2005).

Tendo em mente esta capacidade para com a transmissão de dados, num cenário, hoje isolado é possível criar uma cadeia de Qubits com a informação

desejada onde cada qual carrega uma porção dos dados, mas, conforme é realizada a transmissão pela porta lógica, vão alterando a informação ao longo de sua passagem. Com isso, mesmo que ainda não se tenha produzido de fato um hardware capaz de suportar tais portas lógicas, a capacidade que elas demonstram é inquestionável.

6.Criptografia quântica

6.1.Introdução e funcionamento

Singh (2000) explica que se os computadores atuais tivessem capacidade de verificar um milhão de chaves por segundo para quebrar a cifra DES levariam ainda cerca de mil anos para uma única cifra, enquanto que um computador quântico poderia fazer o mesmo em menos de 4 minutos. Sendo o DES uma das cifras mais usadas atualmente, foi necessário gerar um novo método de criptografia no cenário quântico, surgindo assim a criptografia quântica.

O primeiro a pensar no método de criptografia quântica foi Stephen Wiesner no final da década de 1960, ainda como estudante de graduação na faculdade de Colúmbia, Nova Iorque. Na época, incapaz de conseguir um orientador para seu trabalho sobre um método de impedir falsificação de dólares por uso de polarização de fótons, ele conseguiu lançar seus estudos apenas em 1983 em seu trabalho *Conjugate coding* (Codificação conjugada), onde explica o funcionamento da polarização de fótons, também conhecido como ângulo de vibração do fóton.

Os fótons são capazes de quatro polarizações, horizontal (→), vertical (↑) e as duas diagonais (↘ e ↗). Qualquer lâmpada gera e envia os quatro tipos, porém ao se utilizar um filtro chamado Polaróide, é possível especificar um ou mais tipos de polarização que serão enviadas, controlando-se, assim o tipo de polarização “gerada” pela lâmpada, pois qualquer fóton que seja igual ao filtro passará, e qualquer um diferente, será bloqueado.

Os protocolos da Criptografia Quântica são baseados no princípio de Incerteza de Heisenberg, no fóton que não poderia ter todos os seus estados físicos analisados, uma vez que qualquer um que tente medir o fóton o altera. Há ainda protocolos que se baseiam no Emaranhamento Quântico, nos quais um fóton emaranhado permanece com o emissor e um com o receptor.

6.2.Distribuição de chaves

O primeiro protocolo criado é o BB84, desenvolvido por Charles Bennett e Gilles Brassard em 1984, sendo os sobrenomes dos criadores e o ano a origem de sua nomeação. Este utiliza a polarização de fótons em duas bases, a base retilínea (vertical e horizontal) e a base diagonal (ambas as diagonais). Estas bases são os filtros usados pelo emissor e pelo receptor, como afirmam Singh (2000), Rieznik e Rigolin (2005).

O BB84 já serviu de base para diversos outros protocolos, como o E91 (Ekert 91), BBM92 (Bennett Brassard Mermin 84) e B92 (Bennett 92), mas Rieznik e Rigolin (2005) deixam claro que “mesmo sendo o primeiro protocolo proposto na literatura, ele ainda é, apesar das muitas alternativas de CQ apresentadas a posteriori, aquele de maior importância prática e comercial” (Rieznik, Rigolin, 2005, p. 518).

Este protocolo utiliza-se de um emissor e um receptor, os quais possuem um canal de comunicação quântico e um canal convencional, tomando como base que o convencional possa estar em monitoria de um agente externo. Diante disso, cada membro da comunicação seleciona que tipo de base utilizará, a com polarização horizontal e vertical, ou a com ambas as diagonais, assim como também escolhe qual estado ortogonal em cada base representa um bit 0 e um bit 1, tal como polarização horizontal representa o bit 0 e a vertical o bit 1, o que pode ser feito e comunicado pelo canal convencional.

Dessa maneira, durante a transmissão da chave, o emissor determina a mensagem binária que enviará pelo canal quântico, e seleciona para cada bit qual a base que será utilizada. Uma vez feito isso, os fótons são transmitidos e detectados por bases selecionadas pelo receptor.

Uma vez terminada a transmissão, ambos revelam pelo canal convencional qual base se utilizaram para enviar e detectar os fótons, respectivamente. Como não é revelada a sequência de bits enviados nem os resultados obtidos, o agente externo se mantém incapaz de determinar qual a chave que foi enviada. E, devido

aos princípios da física quântica, caso o mesmo deseje interceptar a transmissão pelo canal quântico, a mensagem será alterada e o agente exterior detectado durante a comunicação entre o emissor e o receptor. Enquanto que se a mensagem de ambos coincidir, significa que a transmissão não foi interceptada e que a mensagem restante é válida como chave para o uso.

Figura 12 – Exemplo de uso do protocolo.

Seqüência de bits de Alice	0	1	1	0	1	1	0	0	1	0	1	1
Bases escolhidas por Alice	B	A	B	A	A	A	A	A	B	B	A	B
Fótons enviados por Alice	$\|0\rangle_B$	$\|1\rangle_A$	$\|1\rangle_B$	$\|0\rangle_A$	$\|1\rangle_A$	$\|1\rangle_A$	$\|0\rangle_A$	$\|0\rangle_A$	$\|1\rangle_B$	$\|0\rangle_B$	$\|1\rangle_A$	$\|1\rangle_B$
Bases escolhidas por Bob	A	B	B	A	A	B	B	A	B	A	B	B
Bits recebidos por Bob	1		1		1	0	0	0		1	1	1
Bob informa fótons detectados	A		B		A	B	B	A		A	B	B
Alice informa bases corretas			OK		OK			OK				OK
Informação compartilhada			1		1			0				1
Bob revela alguns bits da chave					1							
Alice confirma estes bits					OK							
Restante de bits é a chave			1					0				1

Fonte: (RIEZNIK, RIGOLIN, 2005, p. 520)

No exemplo de Rieznik e Rigolin (2005) demonstrado na Figura 12, o emissor Alice e o receptor Bob utilizam o método BB84 para a transmissão de chave. Alice determina a sequência de Bits e a base escolhida a cada um, tendo em mente o que cada posição ortogonal do fóton representa, e Bob determina as suas bases detectoras e recebe uma sequência de bits. Uma vez reveladas por Bob as bases utilizadas, e Alice informando as bases corretas, eles chegam a uma sequência de bits em comum, os quais são utilizados como chave.

Outro protocolo mencionado é o E91, nomeado com o sobrenome de seu criador e ano de criação, o qual utiliza fótons emaranhados, cada um permanecendo com um fóton dos pares emaranhados. Cada um tem seus fótons polarizados e movidos, de forma tridimensional lembrando a esfera de Bloch, e são então medidos de forma que quando ambos “finalizarem as medidas nos vários pares de Qubits oriundos de singletos, eles anunciam publicamente as orientações escolhidas para cada medida e se detectaram ou não seus Qubits” (Rieznik, Rigolin, 2005, pag. 522). É feita então uma triagem dos dados em dois grupos e, caso os resultados obtidos no grupo 1 sejam válidos, ou seja, caso demonstrem que não houve interferência, eles utilizam o grupo 2 para determinar a chave.

O BBM92, nomeado com os sobrenomes de seus criadores e ano de criação, segue de maneira similar ao E91, porém ao invés de usar as três coordenadas da esfera de Bloch, utiliza-se apenas de duas, de forma bidimensional. Uma vez terminado os membros da transmissão,

> anunciam publicamente a orientação de cada polarizador em cada medida. No entanto, eles não informam os resultados. Em seguida, eles descartam todas as medidas nas quais foram utilizadas orientações diferentes. São mantidos apenas os eventos cujos polarizadores foram orientados numa mesma direção (Rieznik, Rigolin, 2005, p. 5232).

E da mesma forma, caso ocorra alguma interferência em um deles, é considerada a possibilidade de um agente exterior, e todo o processo é descartado e reiniciado.

Estes protocolos são os mais considerados até o momento na criptografia quântica uma vez que demonstram segurança na distribuição de chaves, porém mesmo eles possuem suas vulnerabilidades.

7.Estudo de vulnerabilidade

Em 2012, Vadim Makarov do Instituto de Computação Quântica de Waterloo, palestrou sobre os atuais estudos quanto a vulnerabilidades da criptografia quântica. Nesta palestra, ele explicou que a tarefa de um Hacker Quântico é descobrir vulnerabilidades, demonstrar meios de ataques, promover contra medidas e demonstrar suas capacidades de garantir a segurança. Dessa maneira, foram reveladas diversas possibilidades que poderiam ser exploradas por um agente exterior, assim como possíveis soluções.

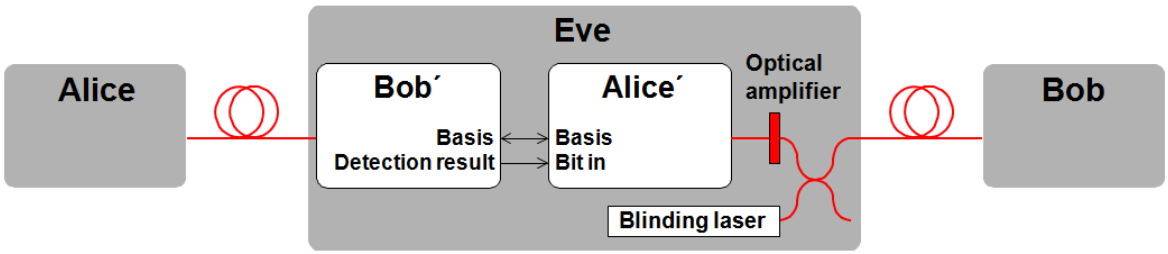
Neste trabalho serão apresentados os métodos APDs, Ataque de tempo morto e Controle por Nanofio supercondutor, bem como a questão do fabricante, também apresentada durante a palestra.

7.1.APDs

As APDs, ou Avalanche Fotodiodo, é o nome de um método de ataque no processo de geração de chaves com criptografia quântica, publicado em 2010 pelo instituto ID Quantique MagiQ Tech, sendo ainda considerado como uma das principais vulnerabilidades neste processo devido a sua simplicidade. O nome é escolhido devido à área do hardware que é explorada, a APD, que é um dispositivo eletrônico semicondutor de alta sensibilidade, com capacidade de converter luz em eletricidade na computação quântica, sendo capaz de converter dados em forma de fótons em dados lógicos. Makarov (2012) descreve que, diante de uma transmissão entre receptor Bob e Emissor Alice, um interceptador Eve implementa no sistema de comunicação um aparelho de espionagem, o qual capta os sinais luminosos enviados pelos fótons emissores de Alice e os interpreta conforme os seus filtros. Simultaneamente, o aparelho de espionagem de Eve se aproveita e emite uma luz constante aos filtros de Bob, o que causa uma cegueira em seus detectores e isso se dá porque, como explica Makarov (2012), dos hardwares atualmente disponíveis para uso em sistemas de distribuição de chaves quântico, o APD é um detector de um único fóton e, ao recebê-lo, ele momentaneamente se torna insensível à recepção de outro fóton, mas não à iluminação. Diante do recebimento de um fóton,

o detector faz um *click*, motivo pelo qual se torna insensível a uma nova detecção de fótons, porém diante de uma iluminação constante, novos *clicks* são feitos, impedindo que o detector se recupere. Com a emissão constante de uma luz, é possível, desta forma, selecionar quando o detector está ativado e quando está incapacitado de receber novos fótons.

Figura 13 – Demonstração do processo de espionagem por meio das APDs.



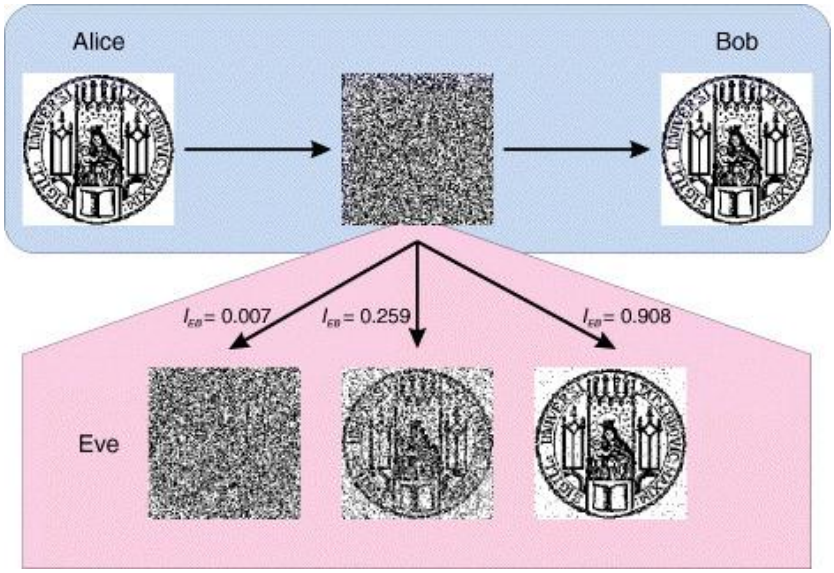
Fonte: (MAKAROV, 2012, slide 30)

Weiner (2011) explica que a capacidade de gerar este controle no detector receptor se dá pela força do pulso utilizado, assim, quanto mais fraca a intensidade do pulso, menor a possibilidade de controle. Porém, quanto maior a intensidade até certo ponto, maior o controle dos detectores até um total, atualmente de 98,83%. Diante deste controle, o aparelho de espionagem de Eve, o qual possui um detector e um emissor, recebe os fótons de Alice, os intercepta e é capaz de retransmitir a Bob, que, por ter seu detector cegado e controlado, é incapaz de perceber a interceptação, como demonstrado na Figura 13. Além disso, enquanto Eve estiver espionando o canal aberto onde os informes das bases são transmitidos, ele é capaz de mais precisamente detectar a chave.

Esta vulnerabilidade no entanto é considerada facilmente combatida. Weiner (2011) explica duas possibilidades de detecção, sendo que devido ao uso deste aparelho de espionagem, a transmissão entre emissor e receptor seria mais demorada, atraindo atenção. O autor explica que esta demora poderia ser reduzida pelo uso de fibras aperfeiçoadas para a computação quântica, mas no momento permanece chamativa, e um receptor atento poderia detectar evidências da

interceptação. Neste caso, o agente exterior poderia ainda implantar diversas luzes cegantes, como mostrado na Figura 14, de modo a parecer que o ataque não passa de ruído na transmissão. Outra possibilidade, e mais efetiva, ele explica, seria a de o receptor verificar a voltagem de seus APDs, uma vez que a luz cegante constante a aumentaria significantemente. Desta forma, se durante a transmissão elas se encontrassem fora do normal, o ataque seria detectado.

Figura 14 – Aplicação do processo de espionagem por APDs com diferentes intensidades no pulso de luz cegante.



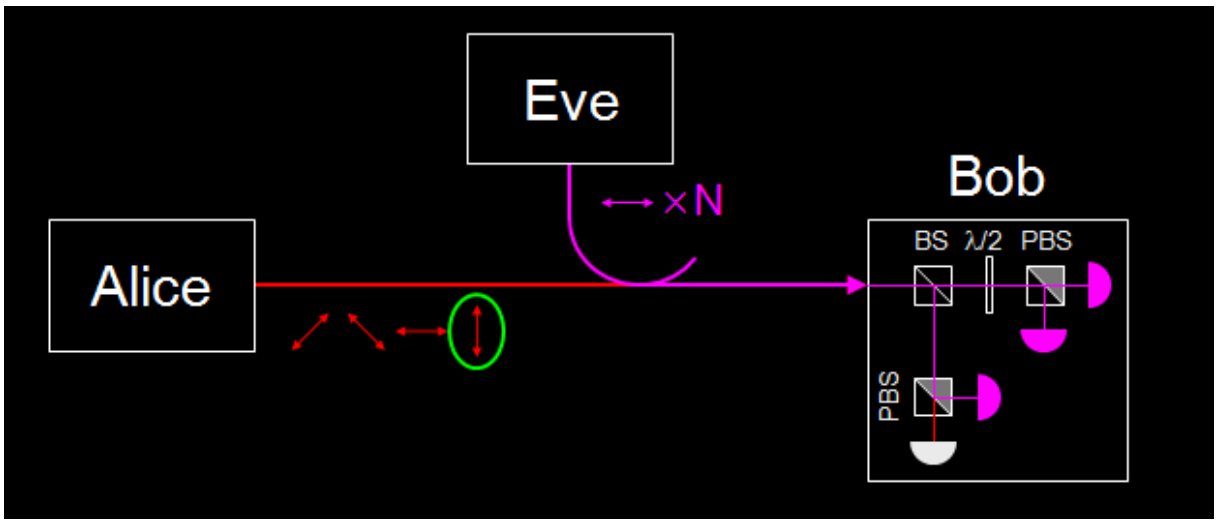
Fonte: (WEINER, 2011)

7.2.Ataque de tempo morto

Outro método de ataque apresentado por Makarov (2012) é o ataque de tempo morto, sendo considerado um processo mais fácil de lidar que o APD. O agente exterior implanta um emissor de sinal na linha de transmissão, porém, sem a presença de um filtro ou qualquer tipo de detector. O agente então emite na transmissão uma enorme quantia de fótons de uma base constante, fazendo com que todos os detectores do receptor recebam, junto aos fótons do emissor, diversos fótons de uma base especifica. Os detectores das demais bases recebem eventualmente fótons de uma base diferente, o que lhes causará uma incapacitação temporária, o *click*. Com isso, a chance destes detectores estarem indisponíveis ao

receber a mensagem original é grande, e a chance de receber apenas os fótons do agente permanece grande, devido à grande quantidade sendo enviada, e isso aumenta a chance da chave final ser baseada unicamente em um tipo de base, o que, junto à espionagem do canal convencional, permite ao agente exterior determinar a chave.

Figura 15 – Demonstração do método de tempo morto.



Fonte: (MAKAROV, 2012, slide 33)

Conforme a Figura 15, os detectores em roxo permanecem incapacitados, enquanto que o detector claro é o único que permanece recebendo sinal. Este processo, no entanto, é considerado possível apenas diante de uma má utilização da transmissão, uma vez que, conforme Makarov (2012) explica, transmissões às quais tenham vários de seus detectores incapacitados diversas vezes deveriam ser encerradas e desconsideradas, uma vez que este cenário é mais facilmente explorável por agentes exteriores. Porém, ainda consideram este ataque válido diante de um cenário de mau uso por parte dos usuários.

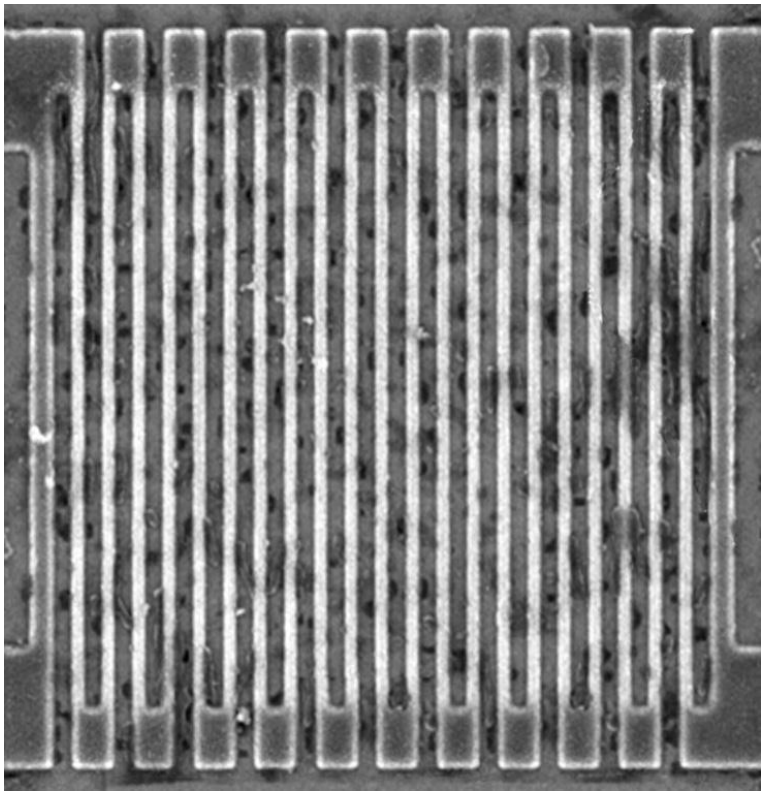
7.3.Controle por Nanofio supercondutor

O método de ataque chamado de Controle de Nanofio supercondutor explicado por Lydersen e Makarov (2011), baseia-se no uso do detector de fótons utilizando nanofio supercondutor, o qual demonstra ser mais rápido que os demais mecanismos de detecção de fótons, porém menos efetivo quando usado para

detecção de fótons em comprimento de onda maior. O fio, com a finura de cinco nanômetros, é esfriado abaixo de sua temperatura critica de supercondutor e mantido com uma corrente elétrica constante. Ele é mantido dobrado e redobrado de forma a criar uma série de paredes entre si, por onde os fótons atravessam, como mostrado da Figura 16. Uma vez que um fóton atravesse a parede do nanofio, a corrente no local é modificada, método como o fóton é detectado e, no local onde este passou, uma resistência é criada, o *hotspot*, o qual permanece incapaz de detectar novamente um fóton por um curto momento.

Desse modo o uso de um laser disparado no nanofio, aquecendo-o e alterando a corrente elétrica no local, gera resistência e logo cria *hotspots* junto à passagem dos fótons, insensibilizando o nanofio de detectá-los. Com isso, assim como no APD, o agente exterior pode então controlar o detector do receptor e, ao se utilizar de uma iluminação em frequência mais curtas e mais luminosas, às quais o nanofio ainda é sensível, o agente pode então escolher o que o receptor recebe por mensagem.

Figura 16 – Imagem do Nanofio supercondutor.



Fonte: (MAKAROV, 2012, slide 37)

Para este método, Lydersen e Makarov (2011) explicam que ainda é discutida uma solução definitiva e isso se deve ao fato de a tecnologia de detecção por nanofio supercondutor ainda ser recente e por tanto, ainda bem vulnerável. Dentre as possibilidades já consideradas, está o uso de um medidor de potência ótica na entrada do sistema receptor, com o qual poderia se detectar a presença de um laser, ou de algum tipo de variação na transição dos fótons. Porém um fator decisivo é o aperfeiçoamento do design do detector por nanofio com foco na segurança e bloqueamento do controle por terceiros.

7.4.Fabricante

Uma questão que Makarov (2012) especifica como sendo de fundamental importância é relacionada aos fabricantes, uma vez que o design dos atuais sistemas utilizados na criptografia quântica é feito sem investimento na segurança ou em métodos para assegurar a detecção de fótons sem interferências. É uma questão justificável, visto que não havia motivo para tais necessidades, porém para que esta tecnologia prossiga, é preciso haver um acompanhamento dos fabricantes destes hardwares para com tais requisitos.

As vulnerabilidades trabalhadas são aquelas já detectadas, mas devido a essa não existência de segurança, não há como supor quantas outras vulnerabilidades ainda não descobertas existem. A criação do design de um hardware com essa preocupação em mente poderia facilitar a detecção de novas vulnerabilidades e o desenvolvimento de novos métodos de prevenção contra as mesmas, porém, essa é uma questão que envolve investimento e confiança nos fabricantes.

8.CONCLUSÃO

Com vista no que foi apresentado, é evidente que a criptografia, assim como todo método de promover segurança à informação, é transponível, seja por um método de criptoanálise, como a descoberta de um padrão para descoberta da chave, seja por falhas humanas, como um usuário que acidentalmente revelar sua senha, ou acidentes diários, como algum incidente que causa redução ou indisponibilidade da proteção e prevenção da informação. Até mesmo a criptografia quântica, com um método de funcionamento teoricamente não interceptável, possui suas falhas que aparecem fora da teoria e a possibilidade de novas falhas que venham a ser descobertas com futuras pesquisas.

A segurança da informação indiscutivelmente sempre possuirá obstáculos, sendo os mais perigosos aqueles ainda a serem descobertos, em especial quando se trata de uma tecnologia ainda em desenvolvimento e aperfeiçoamento, sendo, portanto imprescindível a existência de profissionais voltados à segurança da informação para analisar, estudar e eventualmente saber como lidar com novos incidentes descobertos no dia a dia, mas, além disso, é necessário que trabalhem também na prevenção de tais riscos, seja através do investimento na criação de novos hardwares, de melhores práticas diárias num ambiente profissional ou da análise constante de vulnerabilidades físicas e lógicas em métodos de proteção.

Não há proteção instransponível nesta área, uma vez que há sempre alguém procurando superar tais defesas à informação, seja para ganho próprio, seja para aprimorá-la, como é o caso dos profissionais do Instituto de Computação Quântica de Waterloo. Porém de modo igual, não há método de ameaça à segurança que não possa ser prevenido ou corrigido, diante do trabalho exaustivo, investindo tempo e esforço, daqueles que buscam promover a segurança da informação.

REFERÊNCIAS

BRUMATTO, Hamilton J. **Introdução à Computação Quântica**. Unicamp. 2010. - http://www.ic.unicamp.br/~ducatte/mo401/1s2010/T2/096389-t2.pdf - Acesso em 10/09/2013.

CARVALHO, Luiz, VIRGINIA, Costa. **Representação de um Bit Quântico na Esfera de Bloch.** Cadernos do IME. Série Matemática. Vol. 17. 2005. - http://www.e-publicacoes.uerj.br/index.php/cadmat/article/view/11823/9256 - Acesso em 14/10/2014.

DEUTSCH, David. **Quantum Theory, the Church-turing principle and the Universal Quantum Computer. Proceeding of the Royal society of London**. A 400. Pg. 97-117. 1985

LYDERSEN, Lars, MAKAROV, Vadim, **Controlling a superconducting nanowire single-photon detector using tailored bright illumination**, New Journal of Physics, Vol 13, Novembro 2011 - http://iopscience.iop.org/1367-2630/13/11/113042/ - Acesso em 18/09/2013.

MAKAROV, Vadim. **Palestra sobre Hackeamento Quântico** [Vídeo e slides de apresentação]. Instituto de Computação Quântica de Waterloo, Canada. Junho,2012. - http://www.vad1.com/lab/ - Acesso em 28/08/13.

PESSOA Jr, Osvaldo. **Conceitos de Física Quântica 1**, Volume 1. 1º Edição. Livraria da Física. 2003 - http://books.google.com.br/books?id=cqGAICX7BV0C&lpg=PA37&ots=4o-i7iMKsR&dq=fisica%20quantica&lr&hl=pt-PT&pg=PP1#v=onepage&q&f=false - Acesso em 30/08/13.

RIEZNIK, André A., RIGOLIN, Gustavo. **Introdução a Criptografia Quântica.** Revista Brasileira de Ensino de Física, v. 27, n. 4, p. 517 - 526, 2005 – www.sbfisica.org.br - Acesso em 20/08/13.

SINGH, Simon. **O Livro dos Códigos - A ciência do sigilo - do antigo Egito à criptografia quântica.** Record, 2000.

STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Pratica.** 4º Edição. Pearson, 2007.

WEIER, Henning, **Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors.** New Journal of Physics, vol 13 #7, Julho 2011 - http://iopscience.iop.org/1367-2630/13/7/073024/fulltext/ - Acesso em 18/09/2013.

WIESNER, Stephen**. Conjugate coding.** Sigact News, vol. 15, no. 1, p. 78 – 88, 1983. Originalmente escrito em 1970. - http://dl.acm.org/citation.cfm?id=1008908.1008920 – Acesso em 17/08/2013.